Testimony before the United States House of Representatives

Committee on Veterans' Affairs

Subcommittees on Oversight and Investigations and Technology Modernization

Hearing on "Protecting the Privacy of Veterans' Data"

December 14, 2022

Statement of Harold F. Wolf III

President & Chief Executive Officer

Healthcare Information and Management Systems Society (HIMSS)

Chairmen Pappas and Mrvan, Ranking Members Mann and Rosendale, and Members of the Subcommittees - Thank you for the opportunity to testify today on behalf of the Healthcare Information & Management Systems Society (HIMSS) on the important topic of protecting the privacy of veterans' data.

My name is Harold Wolf, and I am the President and Chief Executive Officer of HIMSS. HIMSS is a global advisor, thought leader, and member-based society committed to reforming the global health ecosystem through the power of information and technology. As a mission-driven non-profit, HIMSS offers a unique depth and breadth of expertise in health innovation, public policy, workforce development, research and analytics to advise global leaders, stakeholders and influencers on best practices in health information and technology. Headquartered in Chicago, Illinois, HIMSS serves the global health information and technology communities with focused operations across North America, Europe, the United Kingdom, the Middle East and Asia Pacific. Our members include more than 120,000 individuals, 480 provider organizations, 470 non-profit partners, and 650 health services organizations across 86 countries.

We appreciate the Committee holding today's hearing on "Protecting the Privacy of Veterans' Data". It's essential that we give our veterans the best possible care while taking all necessary steps to ensure their personal health is kept private and secure within an interoperable health ecosystem. This challenge reflects broader conversations that are occurring across the health ecosystem as we embrace the ongoing digital health transformation journey our country is going through. The goals of privacy and

security are no longer directly in conflict with healthcare delivery and coordination of care. But to ensure the success integration of technological innovation, they must be conceived, built, and maintained with robust privacy, security, and cybersecurity measures to ensure adequate protections.

Before joining HIMSS, I served at The Chartis Group as Director; Practice Leader of Information and Digital Health Strategy, and prior to that I was Senior Vice President and Chief Operating Officer of Kaiser Permanente's The Permanente Federation. During this time, I was responsible for the development and implementation of critical care delivery strategies, data management and governance, population care management environments and the implementation of unique innovations and large-scale programs that impacted end-to-end operations. Critical to the innovations introduced within these functions was maintaining the security and protection of the confidential information entrusted to us by our patients. These responsibilities require the same vigilance in all systems undergoing strategic change.

An Accelerated Digital Health Transformation Driving Data Privacy and Security Considerations

Long before the COVID-19 pandemic, our health ecosystem was undergoing a profound transformation that was increasing pressure on all stakeholders to drive innovation. This digital health transformation has been manifesting in many ways, including expanded use of connected health technologies, the ongoing transition from volume to value-based care, expansion of the health ecosystem, and the gradual adoption and transition to the cloud as the infrastructure supporting this digital health journey/transformation.

The COVID-19 pandemic exposed critical gaps in the health ecosystem and our nation's ability to share vital information, which helped accelerate this transition as we sought ways to respond to the pandemic. When COVID-19 was declared a Public Health Emergency in January 2020, we witnessed rolling shutdowns and government responses across the various jurisdictions and states to limit the spread of COVID-19. No person or sector was immune from these changes, especially healthcare. Seemingly overnight, everything changed.

In response, we saw stakeholders from across the healthcare spectrum quickly adjust to this new dynamic. Prior to the pandemic, telehealth was not widely used or reimbursed; however, out of necessity it became, for a time, a dominant part of healthcare delivery and a key tool supporting access. The rapid adoption of telehealth was supported in part by certain temporary HIPAA waivers that

enabled to use of non-traditional telehealth technologies. Cloud adoption has accelerated in the healthcare sector to keep up with demand. Clinicians, hospital administrators, and patients are all interacting with each other virtually, and "bring your own device" (BYOD) policies were also rapidly adopted to enable clinicians and others to use their mobile devices for work.

The adoption of technology has progressed at such a rapid pace that it now plays a critical role in how we connect and inform clinicians, patients, caregivers, and applications across the health ecosystem. While this transition hasn't always been smooth, we are seeing patients grow more sophisticated in their knowledge of the full health ecosystem, and their ability to understand and act upon the information shared through these technologies.

As we see attention shift to a consumer-based approach regarding integrated care, with greater incorporation of technology into the healthcare setting, we are witnessing more data and information becoming readily available and its access a critical dependency. HIMSS firmly believes that the transition from volume to value-based care, a key objective to realize the goals of improved care outcomes, improved access, and enhanced delivery of care, technology-enabled data collection and interoperable data sharing will play a vital role in supporting these efforts.

Healthcare delivery and coordination of care are best achieved with readily available and reliable data shared in an interoperable and secure manner across disparate systems. Thus, a careful balance must be made between the need to keep the data private and secure, while remaining shareable across various environments to help ensure that patient health and care is not impeded.

The three key components of successful healthcare delivery are the people, processes, and technology. As we've long seen across all of healthcare, technology availability and capabilities have had dynamic and transformative impacts on healthcare achieving the quadruple aim. The same gaps exposed by the pandemic also caused an erosion in the public's trust in key parts of our healthcare system. Ensuring that the people and the processes work in tandem with the technology to support a resilient, secure, and robust health ecosystem while safeguarding patient information will define how effectively care delivery will innovate and help maintain the public's trust. The same holds true for veterans, who have served the U.S. so admirably in defense of our nation. Conversely, poorly designed or integrated systems can contribute directly to provider dissatisfaction and staff burnout. While technology can offer long-term efficiency gains, it cannot substitute for adequate staffing, which VA's REBOOT Task Force identified as the number one concern of VHA staff.

Access to Information is Key for Transformation

As a matter of principle, HIMSS firmly believes that seamless, secure, ubiquitous, and nationwide data access and interoperable health information exchange should ensure the right people have the right access to the right health information in a usable format at the right time to provide the optimal level of care.

We also know that health information and technology serve as the catalyst for transforming the health ecosystem, modernizing care delivery, driving health innovation at the institutional and personal level, and enabling health research.

It is safe to say that there is nothing more personal to an individual than their health information. As we emerge from the pandemic, we continue to be faced with many challenges, but also presented with many opportunities. Reconciling the new reality of increased technology adoption with the growing needs to ensure privacy and security for patients, is critical to the successful transformation of care.

As we look at the healthcare delivery at the VA and across the U.S., enterprise-level leadership must insist that from the very initial stage when technology is developed and introduced, privacy and security principles must be embedded in the planning process. Privacy and security by design occurs during this conceptual stage even before a blueprint is made, and it is important that throughout the product development process it is engineered with robust privacy and security principles in mind. While more innovation is occurring with privacy and security by design, there is nonetheless a tension between the confidentiality, integrity, and availability of the data. Because healthcare involves the sharing of data, such risks are greater since data flows to many different points within an organization and is exchanged with many other business and clinical partners. The need to balance these three elements is critical.

Both before and during the pandemic we saw a significant increase in the use of Internet of Things and the Internet of Medical Things at healthcare organizations and in the hands of consumers. Many devices that were previously simple, standalone devices are now “connected” to networks. These devices, including wearables, are still a relatively nascent technology but their sophistication is growing and the data they produce will have a growing impact on the information clinician and patient alike will utilize. Efforts to enhance the maturity of medical device security to improve data privacy will be a critical step,

including addressing issues such as what and how much data is collected, and where and how the data is stored and later shared.

The drive to move enterprise applications onto the cloud has accelerated across healthcare. Initially, cloud providers were seen as being able to provide better security than the many distributed systems that made up health IT. However, the extreme concentration of services and data onto only a few hyper-scaling cloud providers has proven to be an attractive target for bad actors, and increasingly sophisticated phishing, other social engineering attacks, and more dangerous ransomware will continue to threaten some of the security benefits provided by enterprise clouds. Any strategy that continues to move applications and services to the cloud must take these new threats into account and continue to vigilantly manage the risk posed by social engineering attacks. The added complexity of removing the more predictable physical location of data to the cloud can present additional challenges with jurisdictions, oversight, and different local, regional, and especially international privacy regulations.

However, the concentration of healthcare data in the cloud that we're seeing occur across the healthcare community offers benefits for data accessibility and interoperability. A network architecture based on fewer large-scale, cloud-based nodes should provide for lower-friction data transmission between systems and to authorized applications since fewer robust cloud systems are easier to standardize than many small stand-alone installations of health IT. Nonetheless, it is important for both cloud vendors and cloud customers to understand cloud security fundamentals and appropriately assess and manage risk.

Global Health Data Privacy Policy Landscape

In order to ensure both veterans and broader patient populations receive the best possible care and pathway to health, it's imperative that patients, providers, and caregivers have access to the right information at the right time. Access rights to health data and information with clear usage guidelines are mission critical.

As a global organization, HIMSS offers an unique perspective and thought leadership about the current state of privacy and security across the world. It will be increasingly important to support collaboration between the U.S. government and governments across the globe to help align policies where possible. Any potential alignment will ensure that health related data may be transferred not only based on

consent for the treatment a named patient, but also in a pseudonymized format to allow vital health research to be conducted between the U.S. and its worldwide partners.

The European Union (EU) has enacted a series of legislative changes that are relevant to health data space, including the General Data Protection Regulation (GDPR), which applies to not only entities in the EU but across the globe through its extraterritorial reach (EU GDPR Article 3). Additionally, many countries in the Asia-Pacific region have implemented GDPR-like laws and regulations.

The EU has also recognized the power of data in responding to global pandemics, from contract tracing of infected people, to stock control of limited clinical and medical supplies as well as in driving innovation. In response to the need for timely and accurate data for innovation, the EU established through its Data Governance Act the mechanism for creating of 9 EU data spaces to facilitate data sharing between researchers and innovators, including in countries outside the EU. Recognizing the need to create special legal frameworks for health data, earlier this year the EU released a legislative proposal for the European Health Data Space (EHDS), which seeks to balance the interests of the individual in the privacy of their data with the need for data access by researchers.

While these initiatives take place outside the borders of the U.S., the reach of GDPR and eventually the EHDS will need to be addressed here. If the U.S. doesn't commit to prioritizing a comprehensive privacy framework to harmonize and align the growing patchwork of state and federal regulations, we may ultimately be forced to play catch-up to many of our global partners.

In the United States, HIPAA remains an integral part of our nation's information security and privacy infrastructure for both veterans and broader patient populations. HIPAA has been the prevailing national set of regulatory standards to ensure that patient information is kept both private and secure, and assuring that such health information is available to those who need access to it to provide health care, payment for care, and for other important purposes.

As a result of HIPAA, there is an ever-expanding role for patients and how they contribute to their own personal health journey. Combined with the recently implemented regulations from the Office of the National Coordinator for Health Information Technology (ONC) and the Centers for Medicare & Medicaid Services (CMS), HIPAA contributes to patients accessing and controlling their health information and placing them in a position of greater empowerment to direct their own healthcare.

HIMSS is continuing to work with Congress and across federal agencies to ensure that we are progressing toward a comprehensive health privacy law that applies across the health ecosystem. Federal and state regulations surrounding health data privacy are being revisited, and new ways of thinking about the privacy of an individual's data are being developed in an effort to keep pace with advances in technology.

As new market entrants enter healthcare, how we think about data privacy and security also needs to evolve. How HIPAA applies and intersects with other privacy and security regulations may be an unintended barrier for broader information sharing as well as efforts to better engage patients in their own care and health. The lack of educational awareness as well as the lack of clarity regarding the scope of HIPAA, who is obligated to abide by HIPAA, as well as how it is interpreted, enforced, and intersects with other privacy laws has created significant gaps in compliance and enforcement. Our nation needs a comprehensive health privacy law that encompasses all these issues from a broader perspective and one that is implementable.

Over the last several years there has been rapid change in the technology space, including nefarious activities such as widespread cybersecurity concerns and insider threats. We've also seen efforts in the U.S. to address the digital health regulatory and legal space, which continues to be outpaced by technology change. The United States needs a comprehensive privacy law that accounts for the increasing complexity of security and cybersecurity threats along the lines of what other countries have enacted. Indeed, protecting our veterans' health information is not just a concern for our nation's heroes, but has the potential to become a national security concern.

Addressing Patient Privacy and Security Concerns

In the twenty-plus years that have passed since HIPAA was enacted, we have seen dramatic changes in technology and data usage, as well as an evolution of how we think about data privacy and security. It is important that we continue to focus on the many nuances that the collection and use of a person's individual health data brings into the equation. We often find ourselves overly concerned about questions around data ownership, resulting in a tug-of-war and an unwillingness to share and cooperate. Instead, if our mindset shifts to the governance, access, and appropriate usage of needed data or information to better support individuals and their health outcomes, we can leverage valuable resources on identifying the correct questions and solutions around access and usage.

Robust data governance and organizational governance are both necessary precursors to ensuring the confidentiality, integrity, and availability of information. Good data stewardship focuses on minimizing the risk to patients and to the organization in both the access and use of the data by providing a secure and trackable environment. In today's digital age, data and information drives healthcare. However, information does not exist in a vacuum. It needs to be protected, not just to preserve its privacy, but also to protect the patient and preserve patient safety. Recognizing the value of such information, we need to have robust cybersecurity practices and policies to ensure true interoperability of healthcare data as well. People, processes, and technology need to work in tandem with each other.

As we turn our attention to solutions the VA and the entire health ecosystem can identify and implement, the "whole of organization" approach that includes organizational and data governance, privacy, security, and cybersecurity must be a top priority. The "business" of healthcare must drive the development of solutions, including clear approaches to policies, procedures, and governing body development. As such, cybersecurity risk must be treated as an enterprise-wide matter. Chief Information Security Officers and other cybersecurity professionals may understand the cybersecurity risks, but they may not have the resources or budget to properly address those risks. It is important for the business to drive and enable the effective management of cybersecurity risks. To that end, the entire organization must have a culture of protecting data privacy and cybersecurity and it is important to have appropriate security awareness initiatives and communications to ensure that everyone is aware of what is happening and what to look out for in the future.

The business of healthcare includes the administration, clinical, and operational aspects. Yet, the number one goal of healthcare is to take care of the patients in a safe and effective manner. Accordingly, there is a careful balance in regard to privacy, security, and overall governance. Controls that are draconian or too onerous can result in workarounds that ultimately defeat such controls by end users of organizations. The correlation between patient safety and robust cybersecurity is clear, but access to information is the most essential element. We must find the proper balance between encouraging the free and secure flow of information while preserving and supporting a patient's privacy.

Traditionally, the privacy and security focus of healthcare organizations has been on compliance – which is inherently back-ward looking. Since it was first implemented, HIPAA has played a major part in shaping the privacy and cybersecurity programs at healthcare organizations. Yet, aggressive cyberattacks and increased insider threat activity has also had a growing influence in shaping these

programs. Unfortunately, it is all too common for healthcare organizations to be reactive instead of proactive, and we often find that many healthcare organizations privacy and cybersecurity programs have been shaped through the lens of compliance and thus through a backwards-looking, checklist-based approach.

Yet, threats are necessarily defined as what may happen in the future. Honest mistakes and bad actors are an ever-present threat. Cybersecurity and data privacy are rapidly changing, and we must have programs in place that are forward-looking and stay ahead of any threats to the privacy and security of patient information. At the same time, it is important to not lose sight of known cybersecurity risks that continue to persist. Frequently, threat actors use the same or substantially similar tactics, techniques, and procedures regarding routinely exploited vulnerabilities. It is widely known that many organizations, including those within healthcare, are slow to patch vulnerabilities and upgrade legacy systems and devices. As these threats, intended or otherwise, increase in sophistication and severity, so do the tools and knowledge to combat them.

We believe there are many steps that can be taken to achieve this goal. To start, we believe that cybersecurity and privacy officers need to be at the executive level within their organizations to avoid minimizing an organization's response because threats are "lost in translation." It is necessary for these chief cybersecurity and privacy officers to regularly work with senior leadership peers such as the chief medical information officers, chief nursing information officers, the heads of clinical departments, the heads of administration, the heads of information technology departments, as well as the heads of the procurement, legal, and accounting/finance departments.

Cybersecurity threats are real, and healthcare organization leaders are taking notice. HIMSS is seeing the shifting paradigm toward improved data privacy and security postures throughout the health ecosystem. Through the leadership of our team members and input from healthcare leaders, we are reconsidering the digital maturity models and assessment tools we develop. For example, HIMSS maturity models such as our Infrastructure Adoption model (INFRAM) are undergoing modernization to incorporate the latest in-market and aspirational criteria for assessment, analysis, and strategic planning of all aspects of data security & privacy governance, deployment, and maintenance. This evolution and increased focus on security is in response to the growing voices within the HIMSS membership recognizing this need and asking for assistance, so they can continue doing what they do best: caring for patients.

We must never lose sight of the responsibility to our patients and to our organizations. The diverse array of roles working together brings different and fresh perspectives to running privacy, cybersecurity, and governance programs. For example, procurement, legal, and financial professionals tend to excel in terms of governance, risk, and compliance. Diverse individuals also bring unique perspectives and insights. All of these factors assist with both issue/problem spotting and issue/problem solving which ultimately lead to more resilient and robust organizations.

The Impact of The Department of Veterans Affairs Technology Transformation

The Department of Veterans Affairs is on a technology refreshment journey that, in many ways, mirrors and accelerates a broader shift within US healthcare. As the organization moved from a builder of Information Technology, particularly for their core electronic health record, to a purchaser of technology, there must be a corresponding evolution of workforce skills to ensure industry-leading management techniques are incorporated. Many healthcare systems found their workforces shifting from an informatics research and development focus to one that prioritizes the business management skills of gathering requirements from users and effectively configuring a vendor-provided platform or ensuring that technology and service providers give the necessary priority to incorporating needed changes into their roadmaps. This shift requires a conscious investment in broadening the skills of an existing workforce and can be just as important an investment as dollars spent directly on technology. Given the technological skills and management profiles of today's military community, the VA's hiring practices of hiring veterans and displaced technologists can form a strong foundation for the VA staff readiness to move to the commercial electronic health records (EHR). Veterans and displaced technologists will have a heightened level of security awareness, which could be reenforced by dedicated training.

The sheer scope of VA's IT modernization efforts poses an almost unprecedented management challenge. One 2020 estimate placed the "technical debt" or backlog of systems in dire need of modernization at one billion dollars. Pandemic-related delays and a prolonged rollout of the EHR upgrade have only increased that need over the last two years. The simultaneous convergence of several upgrade strategies may pose unprecedented management challenges. Movement of the core EHR system from in-house to vendor-provided, coupled with a strategy of moving many key administrative systems onto an enterprise cloud opens the door for new integration challenges. We

recommend that the basics of People, Processes, and Technology be considered in depth to ensure efficient investment.

Ensuring Veterans are Protected and Have the Tools to Protect Themselves

It is worth repeating that there is nothing more personal to an individual than their health information. The VA has been a trailblazer in enabling secure access to personal health information. One major contribution was the creation of Blue Button, which has grown into a national initiative. Veterans can access personal health information via MyHealtheVet, built on Blue Button technology. As the VA continues to lead in this space it is vital that patients have meaningful ways in which to request their information, should they want it. This frequently is not communicated. And, even if it is communicated, requests - even when pursuant to HIPAA - are sometimes denied.

The HHS Office for Civil Rights provides guidance for patients regarding their rights to access personal health information. As we move into a digital healthcare delivery system, it is important that we understand patients preferred communication (e.g., via portal, text, call, etc.) and how they access and meaningfully engage with their health information. As digital health platforms such as patient portals continue to evolve, and patients are empowered to consolidate, contribute to, and share their data, patient consent will continue to remain an important cornerstone. Patient consent language needs to be concise and understandable, and the information should not be buried. Additionally, there needs to be controls regarding how data and information is collected, used, and disclosed, that goes beyond consent.

There is no greater goal than ensuring the safety, privacy, and well-being of our veteran population. Similar to the rest of our healthcare system, securing all three is an evolving process. All healthcare organizations are forced to balance a patient's "right-to-access" data and the need to "meet patients where they are" using their technology of choice (or out of necessity) to help reduce access disparities, with a duty to educate and help patients keep their data private.

Although the medium of communication changes frequently, the basic principle that the patient's right to access data, information, and services should not be impeded by any but the gravest privacy concerns is well established in both law and rulemaking. The 21st Century Cures act brought the idea of

"information blocking" to the forefront of our minds and HIPAA addressed this in 2013[1], reminding covered entities that although they have a "duty to warn" patients of the risks of using unencrypted technologies for receiving personal health information, they are not responsible for safeguarding that information once delivered to the individual, and should not allow these technology issues to become a reason to deny information access.

While healthcare organizations must be open to the communications technology that patients choose to use, it is often a best practice to steer or guide them towards safer choices when possible, which the Veterans Health Administration does well. Continuing to promote and enhance products like the My HealtheVet initiative, built on Blue Button technology, provides an important foundation for secure records access.

Veterans should have greater visibility into what kind of information is collected, used, and disclosed about them. This includes protected health information – covered under HIPAA – as well as de-identified information. When such information is de-identified, there needs to be a greater degree of assurance that such information cannot be reidentified. In the future, we should apply differential privacy techniques and algorithms to ensure that veterans' health information and other sensitive information about them is kept both private and secure.

Additionally, many healthcare organizations are applying robust end-to-end encryption to safeguard patient information, including that of our veterans. However, advances in technology – including in quantum computing – presents both threats and opportunities. But it is also essential to understand what the information is that we are protecting today, what the classification of it is (e.g., veterans' patient information, intellectual property, or otherwise), and how it is protected (I.e., which controls are in place). This includes an understanding of what types of encryption are in use today. Obviously, it is more advantageous to use encryption that is state of the art and that has been properly implemented as opposed to something that has already been deprecated or will soon be deprecated.

While all necessary steps must be taken to protect veteran's health data, and ensure their continued safety, privacy, and security, it is equally important to educate veterans, and equip them with additional tools and resources to empower themselves.

[1] Federal Register / Vol. 78, No. 17 / Friday, January 25, 2013, p. 5634

Many healthcare organizations have security awareness programs not just for their staff, but also for their patients. A prime example is the outreach that is done during National Cyber Security Awareness Month, which happens each October. A significant number of healthcare organizations are also going further by ensuring that security awareness programs are conducted year-round. Security, though, does not exist in a vacuum, and privacy and security should and do go hand in hand. As our veterans more frequently access their health information via patient portals using computers, mobile devices, and other electronic means (that are within their capabilities and resources).

While some veterans have cybersecurity backgrounds, others may not. Veterans may understand operational security, but this may or may not extend to robust cyber and privacy hygiene practices. That is why it is essential for all healthcare organizations to ensure that our veterans are equipped with the knowledge and tools to meaningfully contribute to their privacy and security.

In closing, I would like to thank Chairmen Pappas and Mrvan and Ranking Members Mann and Rosendale for this opportunity to testify today, and all members of the Subcommittees for prioritizing such a critical issue. The VA has no greater priority than ensuring that our veterans receive the best possible care, and this cannot be done without ensuring the safety and security of their personal data and health information.